УДК 343.98

Д. И. Шнейдерова
преподаватель кафедры уголовного процесса и криминалистики
Могилевского института МВД Республики Беларусь

ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ПРЕСТУПНИКЕ ПО ДЕЛАМ О ХИЩЕНИЯХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ: КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ

Анализ статистических данных и практики расследования показывает, что киберпреступления занимают лидирующие позиции среди иных групп преступлений как по количеству регистрируемых фактов, так и по низкому уровню раскрываемости и привлечению виновных лиц к уголовной ответственности. К сложившейся ситуации применимо выражение Марка Туллия Цицерона: «Наибольший соблазн преступления заключается в расчете на безнаказанность», — из которого усматривается свойственная киберпреступности пропорциональная зависимость увеличения количества совершаемых преступлений от низких показателей раскрываемости высокотехнологичных преступлений [1].

Хищения, посягающие на криптовалюты как предмет преступления либо совершаемые с использованием криптовалют в качестве средства совершения или сокрытия преступления, составляют отдельную категорию киберпреступлений, имеющую свои специфические особенности ввиду нестандартности объекта исследования. В процессе расследования хищений в сфере оборота криптовалют правоохранительные органы как в рамках работы по материалам проверки, так и по возбужденному уголовному делу взаимодействуют с различными источниками, позволяющими вычленить необходимую информацию, ведущую к изобличению личности преступника. Такие источники можно условно разделить на несколько групп: информация, получаемая от лиц и организаций; информация, фиксируемая при осмотре материальных носителей данных; информация, получаемая при исследовании интернет-ресурсов.

В первую группу входят сведения, получаемые правоохранительными органами при отборе объяснений заявителей, в ходе допросов потерпевших, свидетелей, экспертов, подозреваемых (в отношении их сообщников), по результатам запросов в банковские кредитно-финансовые организации, к операторам мобильных услуг, интернет-провайдерам, учреждениям, осуществляющим операции с криптовалютами (распределительные платформы, криптокошельки, биржи, обменники). Поскольку в большинстве случаев имеют место данные о лице, зарегистрированные в организациях на территории иностранных государств (абонентские номера, банковские карты, IP-адреса устройств, e-mail и т. д.), то для хищений в сфере оборота криптовалют характерно направление запросов об

оказании содействия по материалам проверок (через Национальный контактный пункт МВД), а также международных поручений (просьб) об оказании правовой помощи по уголовным делам (направляются в компетентные органы государств на основе положений норм международных конвенций о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (от 22.01.1993 г., г. Минск; от 07.10.2002 г., г. Кишинев) и Уголовно-процессуального кодекса Республики Беларусь).

При этом следует обратить внимание, что в случае если указанные лица не только дают показания, а организации не только предоставляют ответ на запрос, но и прилагают к этим сведениям соответствующие документы (скриншоты переписок, почтовых писем с одобренными заявками на обменные операции с криптовалютой, выписки из истории транзакций с криптовалютного кошелька, банковские платежные документы, таблицы движения денежных средств по счетам, данные входящего и исходящего интернет-трафика, сведения о телефонных соединениях конкретных абонентских номеров и т. д.) или внешние накопители данных (диски или флеш-карты с вышеуказанной и иной информацией, жесткие диски), то последние следует относить к группе «информация, фиксируемая при осмотре материальных носителей данных». Также к этой категории относятся те предметы — носители информации, которые получены при проведении оперативно-розыскных мероприятий (прилагаются к рапортам) или изъяты органом предварительного расследования в ходе следственных действий (системные блоки, ноутбуки, винчестеры, CD-диски, флеш-карты, SD-карты, мобильные телефоны, планшеты).

Исследование интернет-ресурсов может проводиться в рамках получения справочной информации по уже установленным данным (например, каким провайдером или организацией зарегистрирован установленный IP-адрес устройства, какому мобильному оператору принадлежит абонентский номер и т. д.) либо в ходе осмотра компьютерной информации, где последнему подвергаются аккаунты в социальных сетях и мессенджерах, кабинеты на торговых и игровых площадках, криптокошельки, учетные записи в криптобиржах и обменниках, почтовые ящики, подозрительные сайты, форумы и другие ресурсы.

Работа с источниками своим результатом ставит получение данных, которые могут привести следствие к личности преступника и его местоположению. При этом разновидность и образуемые системы таких данных зависят от вида совершенного хищения и способа его реализации. Так, при вымогательстве криптовалют могут быть установлены: адрес e-mail, ID аккаунта социальной сети, абонентский номер, зарегистрированный в мессенджере, через которые преступник направлял потерпевшему требование о выкупе; адрес криптокошелька, на который необходимо было перевести криптовалюту; IP-адрес устройства, с которого осуществлялся удаленный доступ к компьютеру или мобильному

телефону через сеть Интернет и специализированные программы; веб-ресурс, с которого было загружено вирусное программное обеспечение, и, соответственно, каким хостером он зарегистрирован (т. е. какой организации принадлежит сервер, на котором размещен установленный сайт). Кроме вышеуказанных данных, при мошенничестве с криптовалютой (как направленном на завладение самой криптовалютой, так и денежными средствами, предназначавшимися для ее приобретения или инвестирования) могут быть получены номера банковских карт или электронных кошельков, на которые потерпевшие переводили денежные средства для покупки / обмена криптовалют, абонентские номера, в том числе VoIP и SIP-телефонии, посредством которых осуществлялась связь между сторонами, если имела место личная встреча — описание или изображение лица преступника, номер его транспортного средства (например, при обмене наличных денежных средств нарочно на криптовалюту), адреса веб-страниц, распространявших SCAM-проекты. Хищения путем модификации компьютерной информации сопряжены либо с несанкционированным доступом к криптокошелькам и учетным записям потерпевших на криптобиржах и обменниках, либо с манипуляциями при получении криптовалютного флеш-кредита. В случае несанкционированного доступа могут быть получены сведения об IP-адресах устройств, с которых осуществлялся вход в кошелек или аккаунт, перехват файлов cookie с идентификаторами авторизации, электронных писем, СМС; доменные имена фишинговых веб-страниц, адреса электронной почты, абонентские номера, ID аккаунтов, с которых производилась отправка ссылок на фишинговый ресурс. При манипуляции с флеш-кредитом могут быть получены личные данные кредитополучателя и изображения его лица (как правило, запрашиваются администрацией кредитного ресурса, но их подлинность следует ставить под сомнение), сведения, привязанные к аккаунту (абонентский номер, e-mail, адрес криптокошелька для вывода кредитных средств, банковские платежные карты), данные о криптоплатформах, с которыми взаимодействовал преступник, IP- и MAC-адрес его устройства. Проанализируем способы и средства последующего исследования приведенных данных.

Если в рамках расследования стало известно доменное имя сайта, фишингового или распространяющего вредоносные программы, то информацию о том, каким лицом или организацией был зарегистрирован данный сайт, можно получить у хостинг-провайдера, на сервере которого он размещен, либо у регистратора, зарегистрировавшего доменное имя ресурса (как правило, хостер и регистратор — одна и та же организация), путем направления запроса или международного поручения. Установить данные организации представляется возможным путем использования общедоступных интернет-сервисов Whois, в том числе чат-ботов в Telegram (например, 2ip.ru, whois.net, Iwhois.ru, Reg.ru, Htmlweb.ru и

другие) либо через индексные страницы самого сайта (к доменному имени сайта через слеш добавляется ссылка index.html), которые не во всех случаях будут присутствовать. Ответ на whois-запрос может содержать как наименование организации-регистратора, так и ее контактные данные (телефон, почтовый адрес для связи) либо контактные данные владельца данного доменного имени (такие сведения доступны крайне редко, в основном характерны для сайтов крупных компаний и государственных организаций).

С целью получения информации о лице, на которое зарегистрированы ставшие известными правоохранительным органам абонентский номер или номер банковской платежной карты, необходимо направить запросы обслуживающему мобильному оператору или банку-эмитенту банковской карты, наименования которых можно установить через специальные чат-боты мессенджера Telegram (Quick OSINT, Universal Search) или сервисы в сети Интернет (Pay space magazine, Finanso.com и др.). Кроме того, чат-боты могут предоставлять не только данные об эмитентах, но и интернет-ресурсы, к аккаунтам которых привязан анализируемый мобильный номер или банковская карта. Например, воспользуемся чат-ботом Quick OSINT, которому направим команду на поиск номера мобильного телефона и банковской карты автора. Полученные результаты представлены на рисунке.

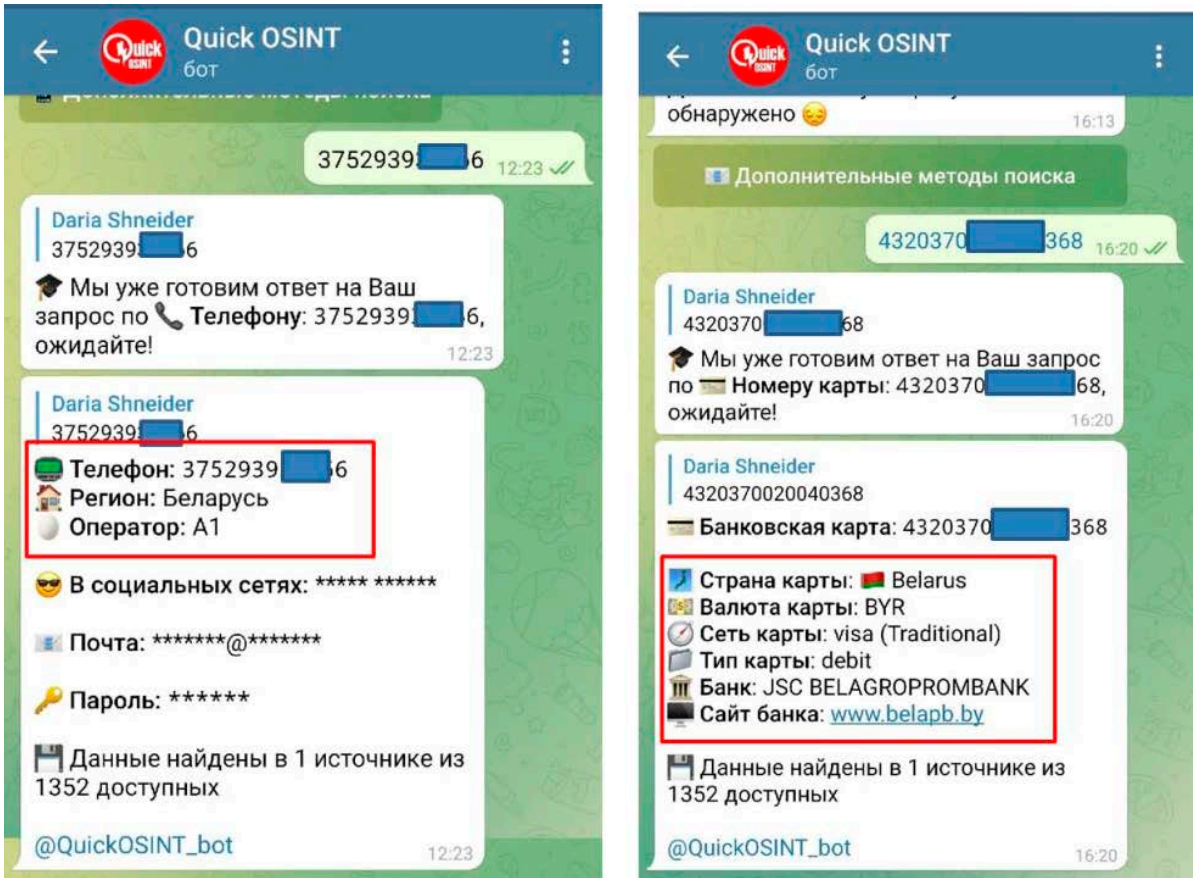

Рисунок — Скриншоты чат-бота Quick OSINT

Установление сведений о лице по адресу электронной почты возможно двумя путями: либо посредством изучения заголовка письма, отправленного преступником потерпевшему; либо, если сообщения отсутствовали и известен только адрес электронного ящика, посредством направления запроса организации-владельцу почтового сервиса. Способ открытия служебного заголовка электронного письма зависит от вида почтового сервиса (подробные инструкции для производства таких действий можно отыскать в свободном доступе в сети Интернет, в том числе в руководстве пользователей почтовых сервисов). В служебном заголовке для правоохранительных органов представляют интерес строки, имеющие заголовки Received: from…, в которых может быть отображен IP-адрес устройства отправителя письма (преступника) в квадратных скобках. Следует учесть, что некоторые атрибуты в служебном заголовке повторяются несколько раз, ввиду чего внимание необходимо обращать на ту строку, которая датируется по времени раньше. Однако не все почтовые операторы размещают в заголовках криминалистически полезную информацию, заполняя эти пробелы своими IP-адресами. В этом случае можно воспользоваться сервисом, позволяющим вычленить из заголовка письма IP-адреса всех серверов, через которые оно прошло (например, Suip.biz, IpTrackeronline.com). Если приведенные данные установить не представится возможным, то следует прибегнуть к запросу организации, владеющей почтовым сервисом, с просьбой о предоставлении информации об IP-адресах, с которых осуществлялся вход в ящик, либо изменялись учетные данные, либо имели место попытки неуспешной авторизации.

IP-адрес — уникальный идентификатор, определяющий устройства, находящиеся в сети. Большинство пользователей полагают, что знание IP-адреса дает стопроцентную гарантию в установлении конкретного человека. Однако на практике это оказывается не так по нескольким причинам: во-первых, опытные пользователи, в том числе и преступники, используют сервисы-анонимайзеры (VPN, SOCKS, TOR, прокси), скрывающие реальные IP и присваивающие устройствам свои адреса, во-вторых, определенные интернет-провайдеры используют технологию трансляции IP-адреса — NAT (присваивает множеству внутренних IP один внешний). Кроме того, целесообразность установления пользователя по вычлененному IP зависит от того, кому он принадлежит: если IP зарегистрирован за проводным или мобильным оператором либо выделен организации, не занимающейся хостингом, то есть вероятность получить положительный результат при направлении запроса; если IP принадлежит хостинг-провайдеру или организации, занимающейся сокрытием IP клиентов, то вероятность получения ответа крайне мала. Для того чтобы выяснить, какая организация (провайдер) владеет конкретным IP, необходимо обратиться к общедоступным интернет-ресурсам, указанным выше для анализа доменного имени

сайта (если ответ на запрос не содержит наименования организации, то следует обратить внимание на почту для связи, через которую осуществлять дальнейшие поисковые действия).

Таким образом, полученные первичные данные требуют дальнейшего анализа для установления личности лица, совершившего преступление, так как физически к человеку могут привести только IP, абонентский номер, номер банковской платежной карты и адрес криптокошелька, если он зарегистрирован на сервисе, соблюдающем требования законодательства о предоставлении таких услуг (т. е. при создании кошелька у пользователя запрашиваются паспортные данные и фотоизображение лица). Такой анализ следует проводить путем поиска справочной информации через общедоступные ресурсы сети Интернет, а также в дальнейшем направления запросов, в том числе международных, к установленным банковским, криптовалютным организациям, мобильным операторам, интернет-провайдерам.

---

1. Афоризмы и цитаты о преступлениях [Электронный ресурс] // Интернет-ресурс Citaty.su. URL: https://citaty.su/aforizmy-i-citaty-o-prestupleniyax (дата обращения: 10.04.2022). Перейти к источнику Вернуться к статье